

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)

Applicant: Tsuneki Takahashi)

Serial No.)

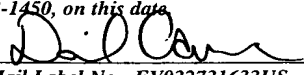
Filed: February 23, 2004)

For: MAGNETIC DISK APPARATUS,)
CIPHER PROCESSING METHOD)
AND PROGRAM)

Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

February 23, 2004
Date


Express Mail Label No.: EV032731633US

CLAIM FOR PRIORITY

Mail Stop PATENT APPLICATION

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-136867, filed May 15, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

Customer No. 24978

GREER, BURNS & CRAIN, LTD.

February 23, 2004
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Phone: (312) 360-0080
Fax: (312) 360-9315

By



Patrick G. Burns

Registration No. 29,367



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 1 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 3 6 8 6 7
Application Number:

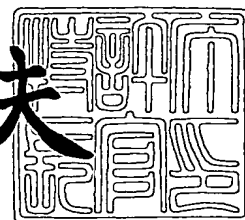
[ST. 10/C]: [J P 2 0 0 3 - 1 3 6 8 6 7]

出 願 人 富 士 通 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 1 2 月 1 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 1 0 4 0 0 9



【書類名】 特許願

【整理番号】 0350393

【提出日】 平成15年 5月15日

【あて先】 特許庁長官殿

【発明の名称】 磁気ディスク装置、暗号処理方法及びプログラム

【請求項の数】 5

【国際特許分類】 G11B 5/09

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 高橋 常樹

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100079359

 【弁理士】

 【氏名又は名称】 竹内 進

【手数料の表示】

 【予納台帳番号】 009287

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9704823

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 磁気ディスク装置、暗号処理方法及びプログラム

【特許請求の範囲】

【請求項1】

データの暗号化と復元に使用する暗号鍵を記憶した暗号鍵記憶部と、
インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて
暗号化して記録媒体に記録させる暗号エンコード部と、
前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記
インタフェースより上位装置にデータを出力させる暗号デコード部と、
前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更部と、
を備えたことを特徴とする磁気ディスク装置。

【請求項2】

請求項1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記記録媒
体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前
記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディス
ク装置。

【請求項3】

請求項1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、上位装置の
コマンド体系以外の特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更す
ることを特徴とする磁気ディスク装置。

【請求項4】

磁気ディスク装置の暗号処理方法に於いて、
データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステッ
プと、



インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる復元読出ステップと、

前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
、
を備えたことを特徴とする磁気ディスク装置の暗号処理方法。

【請求項 5】

磁気ディスク装置に内蔵されたコンピュータに、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】


【発明の属する技術分野】

本発明は、コンピュータを廃棄する際に媒体記録データを喪失させる磁気ディスク装置、暗号処理方法及びプログラムに関し、特に暗号処理を利用して媒体記録データを喪失させる磁気ディスク装置、暗号処理方法及びプログラムに関する。

【0002】

【従来の技術】

従来、使用していたコンピュータを廃棄したり、再利用する場合、磁気ディス



ク装置に記録されているデータの流出を防ぐ必要がある。

【0003】

このような磁気ディスク装置のデータの流出を防ぐ方法としては、データを消去する方法、暗号化データを記録する方法、磁気ディスク装置を物理的に破壊する方法が考えられる。

【0004】

【特許文献1】

特開 2001-092719号

【0005】

【発明が解決しようとする課題】

しかしながら、このような従来の磁気ディスク装置のデータの流出を防ぐ方法は次のような問題点がある。

【0006】

まず磁気ディスク装置のデータ消去には、磁気ディスク装置から完全にデータが消去する場合と、後のデータ復旧を考え OS から見えなくするだけで、データそのものは磁気ディスク装置から消去されない場合がある。

【0007】

しかし、ユーザからはこのようなデータ消去の違いを把握することは難しく、OS から見えなくしただけのデータ消去の場合、データの流出が発生する問題が考えられる。またデータを完全に消去する場合、近年の磁気ディスク装置の大容量化に伴い、全データを消去するのに時間がかかる問題がある。

【0008】

また磁気ディスク装置のデータを暗号化する場合、データと暗号鍵が別々に扱われるため、データが流出しても復元ができないため安全である。しかし、磁気ディスク装置はコンピュータの起動に多用されており、OS まで暗号化することは困難である。

【0009】

即ち、磁気ディスク装置に記録する OS を含む全データを暗号化した場合には

、コンピュータ側に磁気ディスク装置から読み出した暗号データを復元するOSに依存しない専用の暗号復元機能をファームウェア等により設ける必要があり、暗号復元機能をもたないコンピュータでは利用できない。

【0010】

また磁気ディスク装置のデータを暗号化する場合、データと暗号鍵が別々に扱われるため、ユーザに暗号鍵の管理の負担を強いる問題がある。

【0011】

更に、磁気ディスク装置を物理的に破壊する方法は、データの流出を確実に防ぐ事ができるが、動作可能な装置を破壊することになり、装置の再利用が不可能となりコスト的に問題がある。

【0012】

本発明は、暗号化技術を利用して簡単且つ確実にデータ流出を防止する磁気ディスク装置、暗号処理方法及びプログラムを提供することを目的とする。

【0013】

【課題を解決するための手段】

図1は本発明の原理説明図である。本発明の磁気ディスク装置は、データの暗号化と復元に使用する暗号鍵42を記憶した暗号鍵記憶部50と、インタフェースを介して上位装置から入力されたデータを暗号鍵42を用いて暗号化して記録媒体に記録させる暗号エンコード部54と、記録媒体から読み出された暗号データを暗号鍵42を用いて復元してインタフェースより上位装置にデータを出力させる暗号デコード部56と、暗号鍵記憶部50に記憶されている暗号鍵42を変更する暗号鍵変更部58とを備えたことを特徴とする。

【0014】

本発明の磁気ディスク装置では、記録媒体に記録されているデータは暗号化されているため、本発明の磁気ディスク装置を廃棄及び転用する際には、暗号鍵を変更する。このように暗号鍵が変更されると、媒体に記録されている暗号データは変更前の暗号鍵で暗号化されたデータであり、変更後の暗号鍵で復元しても正しいデータは復元されず、無意味なデータが復元されるだけである。このため磁

気ディスク装置に保持している暗号鍵の変更という簡単な操作で、記録領域の全面消去を行うことなく、OSを含む記録領域の全データを破棄することかできる。

【0015】

また本発明の磁気ディスク装置は、データの暗号化及び復元は磁気ディスク装置内で行うため、インタフェースを介したデータは従来の磁気ディスク装置と同じであり、コンピュータ側はOSを含む全てのデータを従来の磁気ディスク装置と同様に扱うことができる。このためコンピュータ側は専用の暗号処理機能を必要としない。

【0016】

また本発明の磁気ディスク装置は、暗号化されたデータと暗号鍵を装置内に格納して運用するため、ユーザは通常の使用では暗号鍵の管理する必要がある。ユーザは、本発明の磁気ディスク装置を廃棄及び転用の際に暗号鍵の変更を行うだけであり、ユーザの暗号鍵の管理に伴う負担を軽減する。

【0017】

更に、本発明の磁気ディスク装置は、データの破棄は暗号鍵の変更によって行うため、暗号鍵を変更した後も装置の機能は失われず、暗号鍵の変更によって磁気ディスク装置は未使用状態に戻り、コンピュータの再利用のためOSのインストールから始めることで、コンピュータを未使用装置として再利用できる。

【0018】

ここで、暗号鍵格納部は、装置の製造段階で書き込まれた所定の暗号鍵を記憶する。暗号鍵記憶部は不揮発メモリを使用する。また、暗号鍵記憶部は記録媒体のユーザ記録領域以外の記録領域としても良い。

【0019】

暗号鍵変更部は、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。暗号鍵変更部は、上位装置のコマンド体系以外の特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。この特殊コマンドはOSに依存しないため、運用中に誤って暗号鍵が変更されることを防止する。

【0020】

暗号鍵変更部は、上位装置にインストールされた暗号鍵変更アプリケーションからの特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。また暗号鍵変更部は、上位装置がネットワークを介してインストールした暗号鍵変更アプリケーションからの特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。

【0021】

このため磁気ディスク装置のデータを破棄する際には、FD等のリムーバル媒体あるいは製造メーカのホームページの参照で提供されるアプリケーションを使用して磁気ディスク装置内の暗号鍵を変更することができ、ユーザにおける暗号鍵の管理は一切不要となる。

【0022】

暗号鍵変更部は、装置内における物理的なイベント操作を認識して、暗号鍵記憶部の暗号鍵を変更する。このように装置内のディップスイッチの操作、特定のピンに対する信号入力、ジャンパ線の切断などの操作を認識して暗号鍵の変更を行うこともできる。

【0023】

暗号鍵変更部は、暗号鍵記憶部に記憶されている暗号鍵の掻き混ぜ処理（シャッフル処理）等より新たな暗号鍵を生成して変更する。また暗号鍵変更部は、暗号鍵記憶部に記憶されている暗号鍵を、上位装置からの暗号鍵変更コマンドに付加された別の暗号鍵に変更するようにしても良い。

【0024】

本発明は、磁気ディスク装置の暗号処理方法を提供する。この暗号処理方法は、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

記録媒体から読み出された暗号データを暗号鍵を用いて復元してインタフェースより上位装置にデータを出力させる復元読出ステップと、

暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を備えたことを特徴とする。

【0025】

ここで暗号鍵変更ステップは、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。

【0026】

本発明は、磁気ディスク装置に内蔵されたコンピュータで実行されるプログラムを提供する。このプログラムは、磁気ディスク装置内蔵のコンピュータに、
データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

記録媒体から読み出された暗号データを暗号鍵を用いて復元してインタフェースより上位装置にデータを出力させる復元読出ステップと、

暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を実行させることを特徴とする。

【0027】

ここで、暗号鍵変更ステップは、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。

【0028】

なお、これ以外の暗号処理方法及びプログラムの詳細は、磁気ディスク装置の装置構成の場合と基本的に同じになる。

【0029】

【発明の実施の形態】

図2は、本発明の暗号処理が適用される磁気ディスク装置のブロック図である。図2において、磁気ディスク装置としてのハードディスクドライブ（HDD）

10は、ディスクエンクロージャ12とコントロールボード14で構成される。ディスクエンクロージャ12にはスピンドルモータ16が設けられ、スピンドルモータ16の回転軸に磁気ディスク媒体20-1, 20-2を装着し、一定速度で回転させる。

【0030】

またディスクエンクロージャ12にはボイスコイルモータ18が設けられ、ボイスコイルモータ18はヘッドアクチュエータのアームの先端にヘッド22-1～22-4を搭載しており、磁気ディスク20-1, 20-2の記録面に対するヘッドの位置決めを行う。尚、ヘッド22-1～22-4にはライトヘッドとリードヘッドが一体化されて搭載されている。

【0031】

ヘッド22-1～22-4はヘッドIC24に対し信号線接続されており、ヘッドIC24は上位装置となるホスト11からのライトコマンドまたはリードコマンドに基づく、ヘッドセレクト信号で書込または読出しを行ういずれかひとつのヘッドを選択する。またヘッドIC24にはライト系については書込アンプが設けられ、リード系についてはプリアンプが設けられている。

【0032】

コントロールボード14にはリードライトLSI26, ハードディスクコントローラ(HDC)28, ホストインタフェース30, SDRAM32, MPU34, フラッシュROM36, VCM/SPMコントローラ38が設けられている。これに加え本発明にあつてはコントロールボード14に暗号処理部40を新たに設けている。

【0033】

また暗号処理部40で使用される暗号鍵42をこの実施形態にあつては、不揮発メモリであるフラッシュROM36に記憶している。フラッシュROM36に対する暗号鍵42の記録は磁気ディスク装置10の製造段階で特殊なコマンドを使用して行われる。

【0034】

ここで磁気ディスク装置10の動作を簡単に説明すると次のようになる。ホス

ト 11 からライトコマンドとライトデータをホストインタフェース 30 で受けると、ライトコマンドを MPU 34 で解読し、必要に応じて転送バッファとして機能する SDRAM 32 のバッファリングを含めて受信したライトデータをハードディスクコントローラ 28 で所定のフォーマットデータに変換すると共に、ECC 符号を付加し、リードライト LSI 26 のライト系でスクランブル、RL 符号変換、更に書込位相補償を行った後、ヘッド IC 24 を介して選択したヘッドのライトヘッドから磁気ディスクに書き込む。

【0035】

この時、MPU 34 から VCM/SPM コントローラ 38 にヘッド位置決め信号が与えられており、ボイスコイルモータ 18 よりヘッドをコマンドで指示された位置に位置決めしている。

【0036】

一方、リード動作はヘッド IC 24 のヘッドセレクトで選択されたリードヘッドから読み出された読出信号をリードライト LSI 26 に入力し、パーシャルレスポンス最尤検出 (PRML) によりリードデータを復調した後、ハードディスクコントローラ 28 で ECC 処理を行ってエラーを検出訂正をした後、転送バッファとしての SDRAM 32 のバッファリングを介してホストインタフェース 30 からリードデータをホスト 11 に転送する。

【0037】

このような磁気ディスク装置 10 におけるライトデータの書込み及びリードデータの読出しにつき本発明にあつては、ホストインタフェース 30 の前段にハードウェアまたはファームウェアの機能により実現される暗号処理部 40 を新たに設けている。

【0038】

暗号処理部 40 はホストインタフェース 30 で受信したライトデータをハードディスクコントローラ 28 に転送する際に、フラッシュ ROM 36 に記憶されている暗号鍵 42 の鍵コード「a1～an」を使用してライトデータを暗号化し、暗号化されたデータをハードディスクコントローラ 28 でフォーマットした後に ECC 符号を付加し、リードライト LSI 26、ヘッド IC 24 を介して

、そのとき選択されているリードヘッドから磁気ディスクに書き込む。

【0039】

一方、磁気ディスク装置から読み出された信号については、ハードディスクコントローラ28より接続される暗号化されているリードデータを暗号処理部40に入力し、フラッシュROM36に記憶している暗号鍵42の鍵コード「a1～an」を使用して暗号データを復号し、復号したリードデータをホストインタフェース30を介してホスト11に転送する。

【0040】

図3は、本発明に適用される磁気ディスク装置の他の実施形態であり、この実施形態にあつては暗号化処理をプログラムにより実行することを特徴とする。即ち図3の実施形態にあつては、図2のハードディスクコントローラ28とホストインタフェース30の間に設けていた暗号処理部40が取り除かれており、その代わりMPU34にプログラムの実行により実現される暗号処理部40を設けている。

【0041】

このようなMPU34の暗号処理部40にあつても、ホストインタフェース30からのライトデータをハードディスクコントローラ28より受けてフラッシュROM36の暗号鍵42のキーコード「a1～an」により暗号化してライト系を介して磁気ディスクに書き込む。

【0042】

また磁気ディスクより書き込まれた暗号化されているリードデータについてはハードディスクコントローラ28から出力する際にMPU34に設けた暗号処理部45によりフラッシュROM36の暗号鍵42の鍵コード「a1～an」を使用して暗号を復元し、復元されたリードデータをホストインタフェース30を介してホスト11に転送する。

【0043】

このように本発明の磁気ディスク装置にあつては、図2のように暗号処理部40をハードウェアで構成するか、図3のように暗号処理部40をプログラムで構成するかは必要に応じて適宜に定めることができる。

【0044】

図4は、本発明の暗号処理部40の機能構成のブロック図である。この暗号処理部40の機能構成は、図2のハードウェアの構成については回路部の機能として実現され、また図3のプログラムの場合にはプログラムの処理機能として実現される。

【0045】

図4において、暗号化処理部40はホストインタフェース30とライトデータ処理部46及びリードデータ処理部48の間に設けられている。ここでライトデータ処理部46は図2及び図3のハードディスクコントローラ28及びリードライトLSI26のライト系をまとめたものであり、一方、リードデータ処理部48は同じくリードライトLSI26とハードディスクコントローラ28におけるリード系をまとめたものである。

【0046】

暗号処理部40は、暗号鍵記憶部50、暗号鍵設定部52、暗号エンコード部54、暗号デコード部56及び暗号鍵変更部58を備える。暗号鍵記憶部50はこの実施形態にあつては、図2及び図3に示した不揮発メモリとしてのフラッシュROM36で実現され、磁気ディスク装置の製造段階に特殊コマンドにより暗号鍵42として鍵コード「a1～an」が予め記憶されている。

【0047】

暗号エンコード部54はホストインタフェース30を介してホスト11から入力されたライトデータを暗号鍵設定部52により設定された暗号鍵記憶部50の暗号鍵42を用いて暗号化し、暗号化されたライトデータをライトデータ処理部46から磁気ディスク媒体に記憶する。

【0048】

暗号デコード部56は磁気ディスク媒体から読み出されたリードデータ処理部48で復唱された暗号化されたリードデータを入力し、暗号鍵設定部52により設定される暗号鍵記憶部50より読み出された暗号鍵42を使用してデータを復元し、ホストインタフェース30から上位ホスト11に復号されたリードデータを転送させる。

【0049】

更に暗号鍵変更部58は本発明の磁気ディスク装置10を搭載したホスト11を廃棄する際に、磁気ディスク装置上のユーザー記憶領域に存在する記憶データを一括して廃棄するために暗号鍵記憶部50に記憶している暗号鍵42の鍵コード「a1～an」を別の鍵コード「b1～bn」を持つ暗号鍵に変更する。

【0050】

この実施形態にあつては暗号鍵変更部58はホスト11側から転送される暗号鍵変更のための特殊コマンドをホストインタフェース30を介して受けることで暗号鍵記憶部50の暗号鍵42の変更を実行する。

【0051】

暗号鍵変更部58に対するホスト11からの暗号鍵変更のための特殊コマンドは、例えば本発明の磁気ディスク装置の製造段階で使用する特殊なコマンドであり、ホスト11のOSに依存することがなく、従って運用中においてホストのOSからのコマンドによって暗号鍵記憶部50の暗号鍵42の変更されることはない。

【0052】

ここで本発明の暗号処理部40で使用する暗号としては、例えば次のようなものがある。

【0053】

(1) DES

DES暗号は1977年にアメリカ商務省標準局(NBS)がデータ暗号化規格(Data Encryption Standard)を公募したときにIBM(R)から提出された方式に修正が加えられたものである。DES暗号は、データを1ブロック64ビットとして扱い、暗号鍵は7バイトの鍵データと1バイトの奇数パリティから成り立っている。

【0054】

(2) CAST-128

CAST-128暗号は、エントラスト・テクノロジー社(Entrust Technologies)のカルロス・アダムス(Carlisle Ada

ms) とスタッフォード・トラバース (Stafford Traverses) によって開発されたブロック暗号である。ブロック長は64ビット、鍵長は1～128ビット可変となっており、12～16ラウンドで処理される。このアルゴリズムには特許が成立しているが、フリーで使用できることが明言されており、RFC 2144として公開されている。

【0055】

(3) その他、ISO/IEC 9979に登録されている暗号アルゴリズム
本発明の暗号処理部40にあっては前述した暗号のアルゴリズムをそのまま適用しても良いし、暗号鍵変更部58でライトデータにランダムな冗長を付加した後に、例えばDESアルゴリズムなどにより暗号化し、リードデータについては暗号デコード部56でDESアルゴリズムなどで復号した後に冗長分を切り捨ててデータを出力しても良い。

【0056】

このようにデータを暗号化する際にランダムな冗長を付加することで暗号が万一解読された場合にも冗長データで無意味なデータとなっていることで安全性を更に高めることができる。

【0057】

図5は、図4の暗号処理部40による処理手順を示したフローチャートである。このフローチャートは図3のMPU34に設けている暗号処理部44を実現するプログラムの処理手順を同時に表している。この暗号処理の手順は本発明の磁気ディスク装置のパワーオンスタートにより実行され、次の処理手順からなる。

【0058】

ステップS1：暗号鍵記憶部となる不揮発メモリから予め記憶されている暗号鍵の鍵コード「a1～an」を読み出して暗号エンコード部54と暗号デコード部56に設定する。

ステップS2：ライトアクセスをチェックし、ホスト11からライトコマンド及びライトデータが転送されるライトアクセスであればステップS3に進み、そうでなければステップS4に進む。

ステップS3：ライトデータを暗号鍵の鍵コード「a1～an」により暗号デー

タに変換してハードディスクコントローラ 28 側に転送して、磁気ディスク媒体に書き込む。

ステップ S 4：リードアクセスか否かチェックし、リードコマンドによるリードアクセスであればステップ 5 に進み、そうでなければステップ S 6 に進む。

ステップ S 5：ハードディスクコントローラから出力された暗号化されているリードデータを暗号鍵の鍵コード「a 1～a n」を使用して解読して、ホストインタフェース 30 からホスト 11 に転送される。

ステップ S 6：暗号鍵変更コマンドの受信をチェックしており、コマンドを受信するとステップ S 7 に進み、そうでなければステップ S 2 に戻る。

ステップ S 7：不揮発メモリから暗号鍵の鍵コード「a 1～a n」を読み出す。

ステップ S 8：ホスト 11 から受信した暗号鍵変更コマンド（特殊コマンド）により不揮発メモリの暗号鍵の鍵コード「a 1～a n」を別の暗号鍵となる鍵コード、例えば鍵コード「b 1～b n」に変更する。この暗号鍵の変更は

- (1) 暗号鍵変更コマンドに付加された暗号鍵へ変更、
 - (2) 現在に暗号鍵をシャッフルなどにより処理して別の暗号鍵へ変更、
- となる。

ステップ S 9：不揮発メモリの暗号鍵を変更した暗号鍵に書き替える。

【0059】

尚、ステップ S 8 の暗号鍵の変更処理におけるシャッフルとしては変更前の暗号鍵の鍵コード「a 1～a n」に対し、ランダムにビットを反転をしたり、例えばバイト単位に分割して位置を入れ替えたり、更にはバイト分割をして位置を入れ替えて元の鍵コードとの排他論理和をとるなど適宜のシャッフルが適用できる。即ち、本発明における暗号鍵の変更は、変更前の暗号鍵が失われ、変更前とは異なる新たな変更鍵ができるものであれば変更の手法は問わない。

【0060】

図 6 は、本発明の磁気ディスク装置に対する暗号鍵変更ツールを提供するネットワーク環境の説明図である。図 6 において、本発明の磁気ディスク装置 10 を搭載したユーザコンピュータ 60 を廃棄させる場合、ユーザコンピュータ（ホスト）60 の WWW ブラウザ 62 を使用して、インターネット 66 上の例えば製造

元サーバ64から暗号鍵変更用のツールをダウンロードして実行させることができる。

【0061】

このため製造元サーバ64には、WWWサーバ68、HDD廃棄管理部70、ユーザ管理ファイル72及び暗号鍵変更アプリケーションファイル74が設けられている。

【0062】

図7は、図6のユーザ管理ファイル72の一例であり、管理ID、コンピュータ番号、ハードディスク番号をコンピュータの製造段階で作成して登録しており、更に暗号鍵変更フラグが設けられ、変更がなければフラグは0であり、ユーザからの要求で暗号鍵変更アプリケーションファイル74からの暗号鍵変更ツールのダウンロードによる変更が行われるとフラグは1にセットされる。

【0063】

この例では管理IDが「0300004」について暗号鍵変更フラグが「1」にセットされて暗号鍵変更処理が行われたことが示されており、このコンピュータは廃棄されるか、別のユーザにより再利用されていることになる。

【0064】

図8は、図6の製造元サーバ64にユーザコンピュータ60のWWWブラウザ62でアクセスした際に表示されるハードディスク廃棄ツール操作画面75の説明図である。

【0065】

このハードディスク廃棄ツール操作画面75において、「ハードディスク廃棄ツールをインストールしますか」の表示に対し、「はい」のチェックボックスをクリックしてOKボタン77を操作するとユーザコンピュータ60において製造元サーバからダウンロードされたハードディスク廃棄ツールが実行され、磁気ディスク装置10に記憶している暗号鍵を変更するための特殊コマンドが発行され、暗号鍵の変更が行われる。

【0066】

このようにして一度磁気ディスク装置10の暗号鍵を変更してしまうと、変更

後にユーザコンピュータ 60 の電源を落として停止し、再度電源を投入したときには暗号鍵が変更されているため、その時、磁気ディスク媒体に記憶している OS を含む全データは変更後の暗号鍵で解読されることとなり、暗号鍵が違うことにより全く無意味なデータが解読されることになり、結果として磁気ディスク装置の読出しによる OS の立上りはできず、ユーザコンピュータ 60 は OS をインストールしていない全く未使用状態と同じ状態になる。

【0067】

このためユーザコンピュータを廃棄した場合、第三者が廃棄されたユーザコンピュータを起動してもユーザコンピュータは全く動作せず、データの流出は起きない。

【0068】

またユーザコンピュータを分解して磁気ディスク装置の暗号鍵を何らかの操作で入手したとしても、磁気ディスク媒体に記憶されているデータはすでに失われている変更前の暗号鍵により暗号化されたデータであり、この時、取得した暗号鍵によっては復元することはできず、変更後の暗号鍵がわかったとしてもデータの流出することはない。

【0069】

一方、暗号鍵の変更を実行して廃棄したユーザコンピュータを別のユーザが再利用する際には、全く使用されていない新品のコンピュータと同様、OS のインストールを行って磁気ディスク媒体の暗号化された OS を記憶すれば、それ以降の処理は変更後の暗号鍵に従った暗号化と復元化が行われ、通常の暗号化処理を行ってないユーザコンピュータと同等に利用することができる。

【0070】

また図 6 のようなネットワーク上からハードディスク廃棄ツールを取得してユーザコンピュータ 60 に搭載している磁気ディスク装置 10 の暗号鍵を変更することができるため、ユーザにおいて暗号鍵の管理は一切必要なく、ユーザコンピュータ 60 を廃棄する際のひとつの手順としてネットワーク上からハードディスク廃棄ツールを取得してそれを実行すればよい。

【0071】

このようなハードディスク廃棄ツールをユーザに提供する別の手法としてフロッピーディスク（R）などに格納してユーザに提供することも可能であるが、この場合、ネットワーク上から取得するほうが媒体の管理を必要としない分、簡単かつ確実に利用できる。

【0072】

図9は、装置内の物理的な操作により暗号鍵を変更する本発明の他の実施形態にブロック図である。この実施形態にあつては暗号処理部40に対し磁気ディスク装置内に変更操作部位76を設けている。変更操作部位76としては図2及び図3におけるコントロールボード14上に設けているディップスイッチ、信号入力ピン、切断により操作入力を行うジャンパ線など、適宜の物理的な操作部位を用いることができる。

【0073】

変更操作部位76の物理的な操作が行われると、暗号鍵変更部58に対しイベント入力が行われ、このイベント入力は暗号鍵変更部58を動作する特殊コマンドと同等の機能をもっており、これにより暗号鍵変更部58は暗号鍵記憶部50に記憶している暗号鍵42の鍵コード「a1～an」を例えば「b1～bn」といった別の鍵コードに変更する。

【0074】

この場合の鍵コードの変更は別の暗号鍵の鍵コードを予め記憶しておくことは安全でないことから、変更前の暗号鍵の鍵コード「a1～an」をシャッフルなどの動作により別の鍵コードに変更する暗号鍵の変更が望ましい。

【0075】

図10は、暗号鍵を磁気ディスク媒体に格納した本発明の他の実施形態のブロック図である。図10において、暗号鍵42は磁気ディスク媒体20-1におけるユーザ記憶領域以外の記録領域、具体的には磁気ディスク装置の製造段階で各種のパラメータの格納に使用するいわゆるシステム領域に暗号鍵42を記憶している。

【0076】

このような磁気ディスク媒体20-1に対する暗号鍵42の格納に対応して暗

号処理部 40 は暗号鍵読出書込部 78 が設けられている。暗号鍵読出書込部 78 は磁気ディスク装置をパワーオンスタート時にリードデータ処理部 48 を介して磁気ディスク媒体 20-1 のシステム領域に格納されている暗号鍵 42 を読み出して、暗号エンコード部 54 及び暗号デコード部 56 に設定する。

【0077】

またこの実施形態ではホストインタフェース 30 を介してホスト 11 側より暗号鍵変更のための特殊コマンドが与えられると、暗号鍵変更部 58 は暗号鍵読出書込部 78 のリード動作により磁気ディスク媒体 20-1 から暗号鍵 42 を読出し、これを変更後の暗号鍵に書き替え、ライトデータ処理部 46 から磁気ディスク媒体 20-1 のシステム領域に書き込んで暗号鍵を変更する。

【0078】

図 11 は、図 10 と同じ暗号鍵を磁気ディスク媒体に格納する場合について暗号鍵の変更を装置内の変更操作部位 76 により行う本発明の他の実施形態のブロック図である。

【0079】

この場合の変更操作部位 76 は、図 9 の実施形態と同様、図 2 及び図 3 のコントロールボード 14 側に設けられたディップスイッチ、信号入力ピン、切断により操作入力を行うジャンパ線などの適宜の物理的な操作部位が用いられている。

【0080】

尚、上記の実施形態にあつては、暗号処理部 40 をホストインタフェース 30 とハードディスクコントローラ 28 の間に設けてデータにの暗号化と復号を実行しているが、暗号処理部 40 をハードディスクコントローラ 28 とリードライト LSI 26 の間に設け、磁気ディスク媒体に対する記憶読出しのためのフォーマット済みのデータに対し、暗号処理を行うようにしても良い。

【0081】

即ち本発明にあつては磁気ディスク媒体に記憶する前であれば適宜の段階で暗号化しても良く、また磁気ディスク媒体からの読出しについても読出し後のデータがあれば適宜の位置で暗号データの復元を行ってもよい。

【0082】

また本発明はその目的と利点を損なわない適宜の変形を含み、更に上記の実施形態に示した数値による限定は受けない。

【 0 0 8 3 】

ここで本発明の特徴を列挙すると次の付記のようになる。

(付記)

(付記1)

データの暗号化と復元に使用する暗号鍵を記憶した暗号鍵記憶部と、
インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号化して記録媒体に記録させる暗号エンコード部と、
前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる暗号デコード部と、
前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更部と、
を備えたことを特徴とする磁気ディスク装置。(1)

【 0 0 8 4 】

(付記2)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は、装置の製造段階で書き込まれた所定の暗号鍵を記憶することを特徴とする磁気ディスク装置。

【 0 0 8 5 】

(付記3)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は不揮発メモリであることを特徴とする磁気ディスク装置。

【 0 0 8 6 】

(付記4)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は記録媒体のユーザ記録領域以外の媒体領域であることを特徴とする磁気ディスク装置。

【 0 0 8 7 】

(付記5)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記

暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディスク装置。(2)

【0088】

(付記6)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、上位装置のコマンド体系以外の特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。(3)

【0089】

(付記7)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記上位装置にインストールされた暗号鍵変更アプリケーションからの特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【0090】

(付記8)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記上位装置がネットワークを介してインストールした暗号鍵変更アプリケーションからの特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【0091】

(付記9)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、装置内における物理的なイベント操作を認識して、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【0092】

(付記10)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記暗号鍵記憶部に記憶されている暗号鍵の掻き混ぜ等の処理のより新たな暗号鍵を生成して変更することを特徴とする磁気ディスク装置。

【0093】

(付記 11)

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記暗号鍵記憶部に記憶されている暗号鍵を、上位装置からの暗号鍵変更コマンドに付加された別の暗号鍵に変更することを特徴とする磁気ディスク装置。

【0094】

(付記 12)

磁気ディスク装置の暗号処理方法に於いて、
データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、
インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、
前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる復元読出ステップと、
前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を備えたことを特徴とする磁気ディスク装置の暗号処理方法。(4)

【0095】

(付記 13)

付記 12 記載の磁気ディスク装置の暗号処理方法に於いて、前記暗号鍵変更ステップは、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディスク装置の暗号処理方法。

【0096】

(付記 14)

磁気ディスク装置に内蔵されたコンピュータに、
データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、
インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、
前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記イ

インタフェースより上位装置にデータを出力させる復元読出ステップと、前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、を実行させることを特徴とするプログラム。(5)

【0097】

(付記15)

付記14記載のプログラムに於いて、前記暗号鍵変更ステップは、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とするプログラム。

【0098】

【発明の効果】

以上説明してきたように本発明によれば、磁気ディスク装置内に記憶保持している暗号鍵を変更するだけで記憶媒体上のデータを破棄することができ、時間のかかる記憶媒体のデータ領域の全面消去を行うことなく、データの流出が確実に防止でき、データの破棄を容易に行うことができる。

【0099】

また本発明にあつては装置内、例えばインタフェース部分で書込みの際のデータの暗号化と読出しの際の暗号データを復元を行うため、インタフェースの外側に位置するホスト側は本発明の磁気ディスク装置における暗号処理を意識する必要がなく、従来の磁気ディスク装置と同等に扱うことができ、本発明の磁気ディスク装置は暗号処理を内蔵していても従来の磁気ディスク装置と同等に置き換えることができる。

【0100】

また暗号鍵を変更して破棄された本発明の磁気ディスク装置の不揮発メモリあるいは記憶媒体より暗号鍵を取り出して記憶媒体のデータを読み出した場合にあつても、記憶媒体のデータは変更前の暗号鍵で暗号化されたデータであり、取り出した暗号鍵は変更後であるため、暗号鍵を使用しても記憶媒体の暗号データは復元できず、データの安全性が完全に保証される。

【0101】

また本発明の磁気ディスク装置は暗号化されたデータと暗号鍵を装置内に格納しているため、ユーザは通常の使用において暗号鍵を管理する必要がなく、暗号鍵に対するユーザの負担は生じない。

【0102】

更に暗号鍵を変更すると磁気ディスク装置が未使用状態に戻ることであり、ホストにおけるOSのインストールにより再使用ができる。

【図面の簡単な説明】**【図1】**

本発明の原理説明図

【図2】

ハードウェアで暗号処理を行う本発明による磁気ディスク装置のブロック図

【図3】

プログラムで暗号処理を行う本発明による磁気ディスク装置のブロック図

【図4】

本発明によるプログラム暗号処理の機能構成のブロック図

【図5】

本発明における暗号処理のフローチャート

【図6】

本発明の磁気ディスク装置に対し暗号鍵変更ツールを提供するネットワーク環境の説明図

【図7】

図6の製造元サーバにおけるユーザ管理ファイルの説明図

【図8】

図6のブラウザにインストールしたハードディスク廃棄ツールの操作画面の説明図

【図9】

装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック

図

【図 10】

暗号鍵を記録媒体に格納した本発明の他の実施形態のブロック図

【図 11】

暗号鍵を記録媒体に格納し装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図

【符号の説明】

- 10：ハードディスクドライブ（HDD）
- 11：ホスト
- 12：ディスクアッセンブリ
- 14：コントロールボード
- 16：スピンドルモータ（SPM）
- 18：ボイスコイルモータ（VCM）
- 20，20-1，20-2：磁気ディスク媒体
- 22-1～22-4：ヘッド
- 24：ヘッドIC
- 26：リードライトLSI
- 28：ハードディスクコントローラ（HDC）
- 30：ホストインタフェース
- 32：SDRAM
- 34：MPU
- 36：フラッシュROM
- 38：VCM／SPMコントローラ
- 40：暗号処理部
- 42：暗号鍵
- 44：スクランブル回路
- 46：ライトデータ処理部
- 48：リードデータ処理部

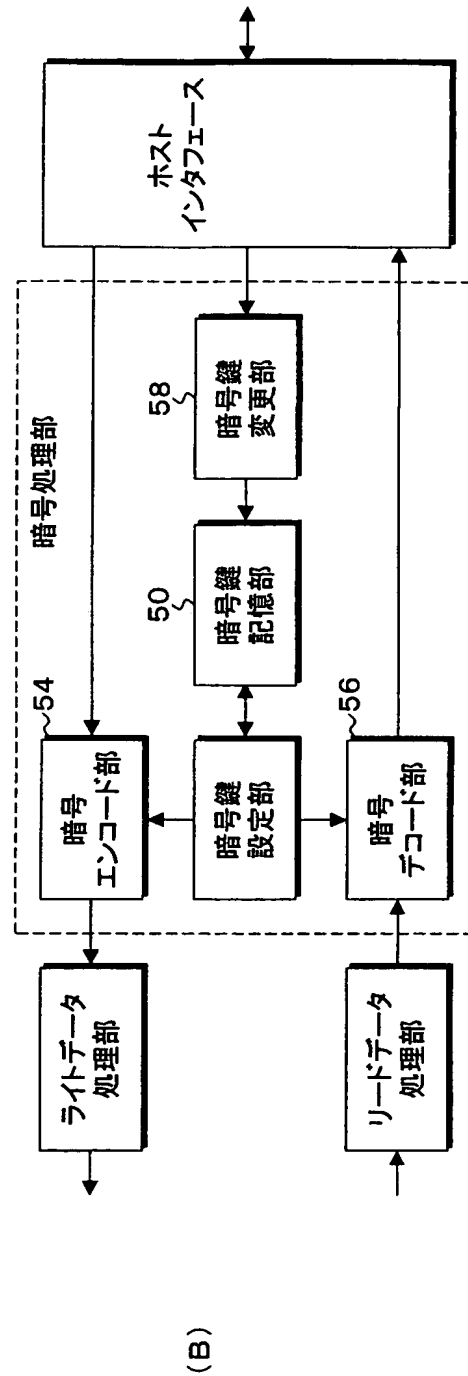
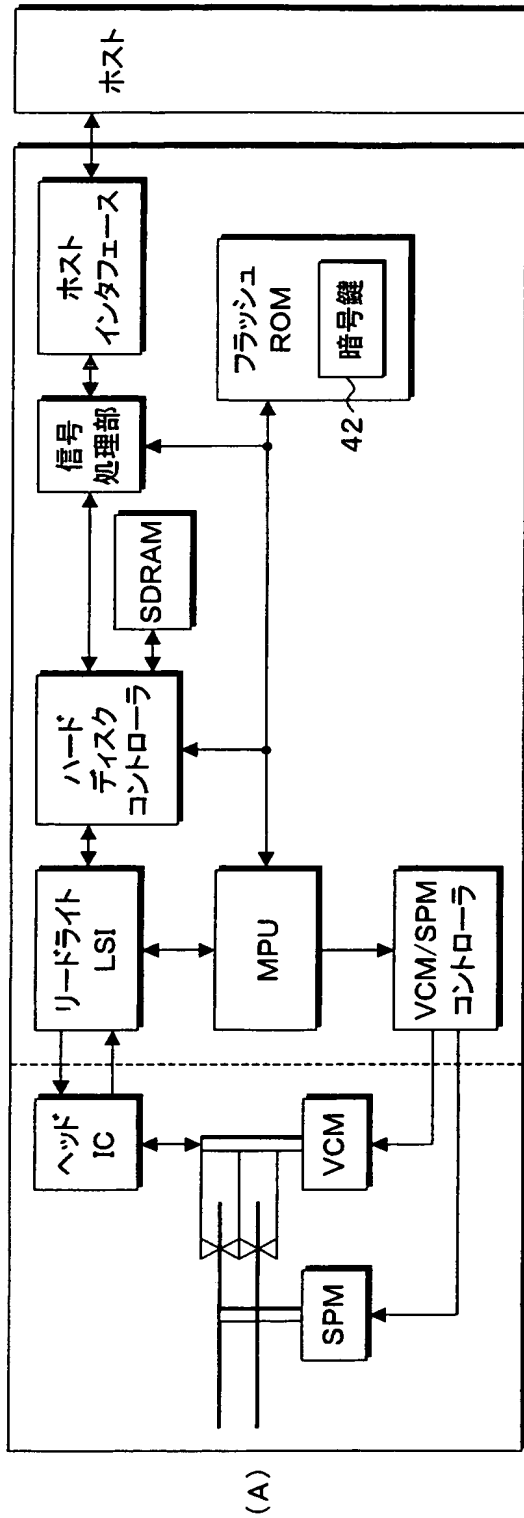
5 0 : 暗号鍵記憶部
5 2 : 暗号鍵設定部
5 4 : 暗号エンコード部
5 6 : 暗号デコード部
5 8 : 暗号鍵変更部
6 0 : ユーザコンピュータ
6 2 : WWWブラウザ
6 4 : 製造元サーバ
6 6 : インターネット
6 8 : WWWサーバ
7 0 : HDD廃棄管理部
7 2 : ユーザ管理ファイル
7 5 : ハードディスク廃棄ツール操作画面
7 4 : 暗号鍵変更アプリケーションファイル
7 6 : 変更操作部位
7 7 : OKボタン
7 8 : 暗号鍵読出書込部
8 0 : ライトヘッド
8 2 : リードヘッド

【書類名】

図面

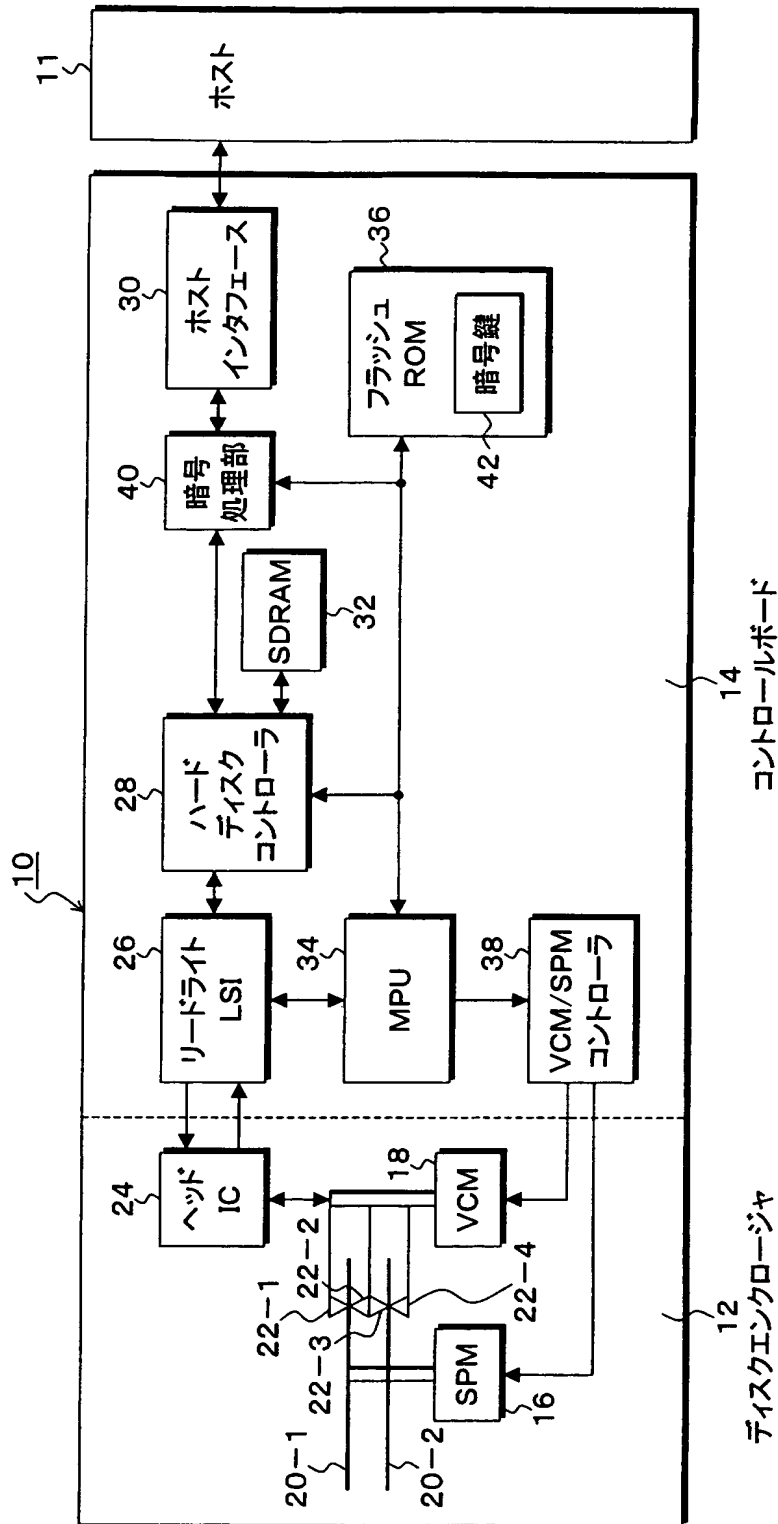
【図 1】

本発明の原理説明図



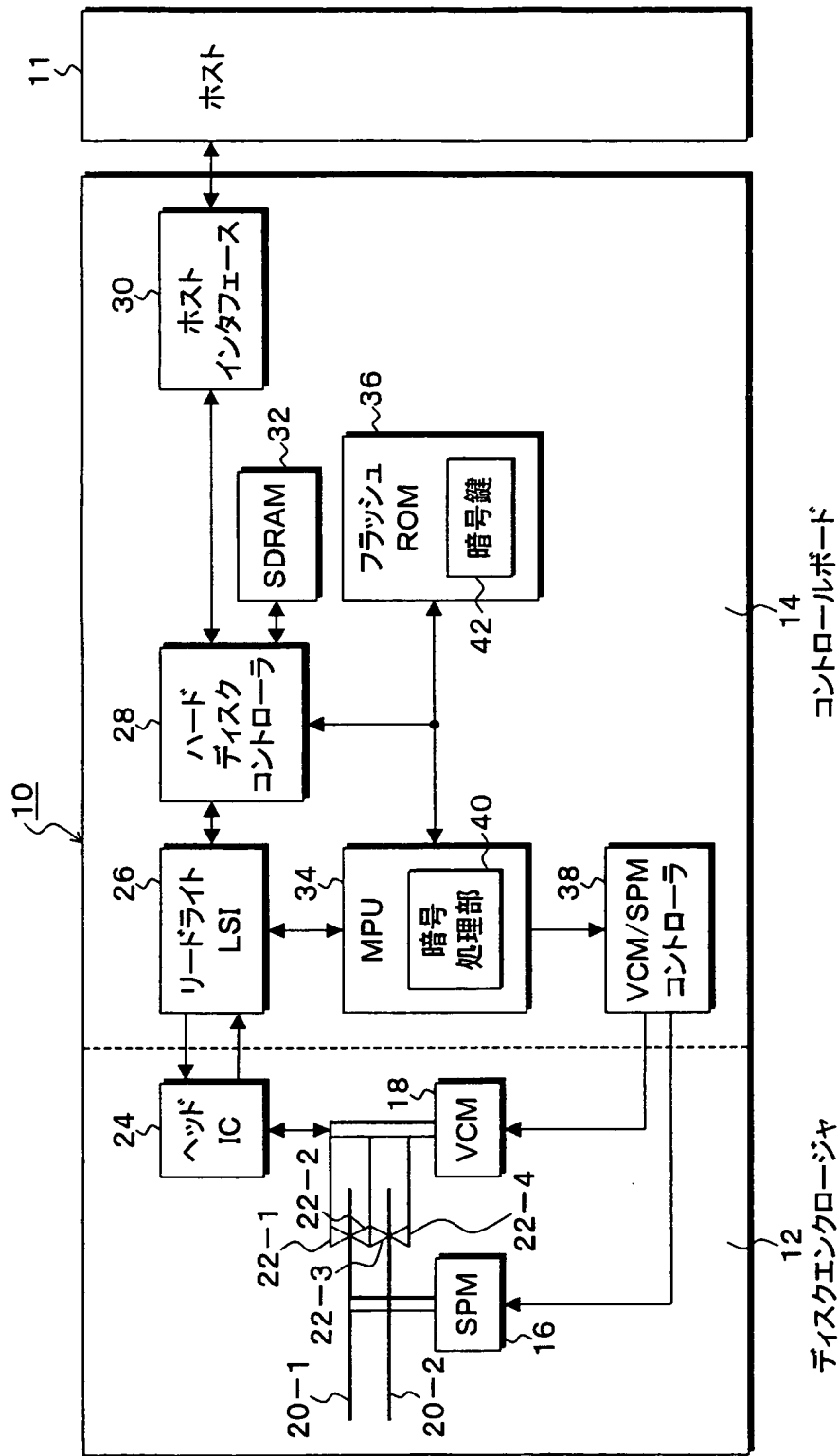
【図 2】

ハードウェアで暗号処理を行う本発明による磁気ディスク装置のブロック図



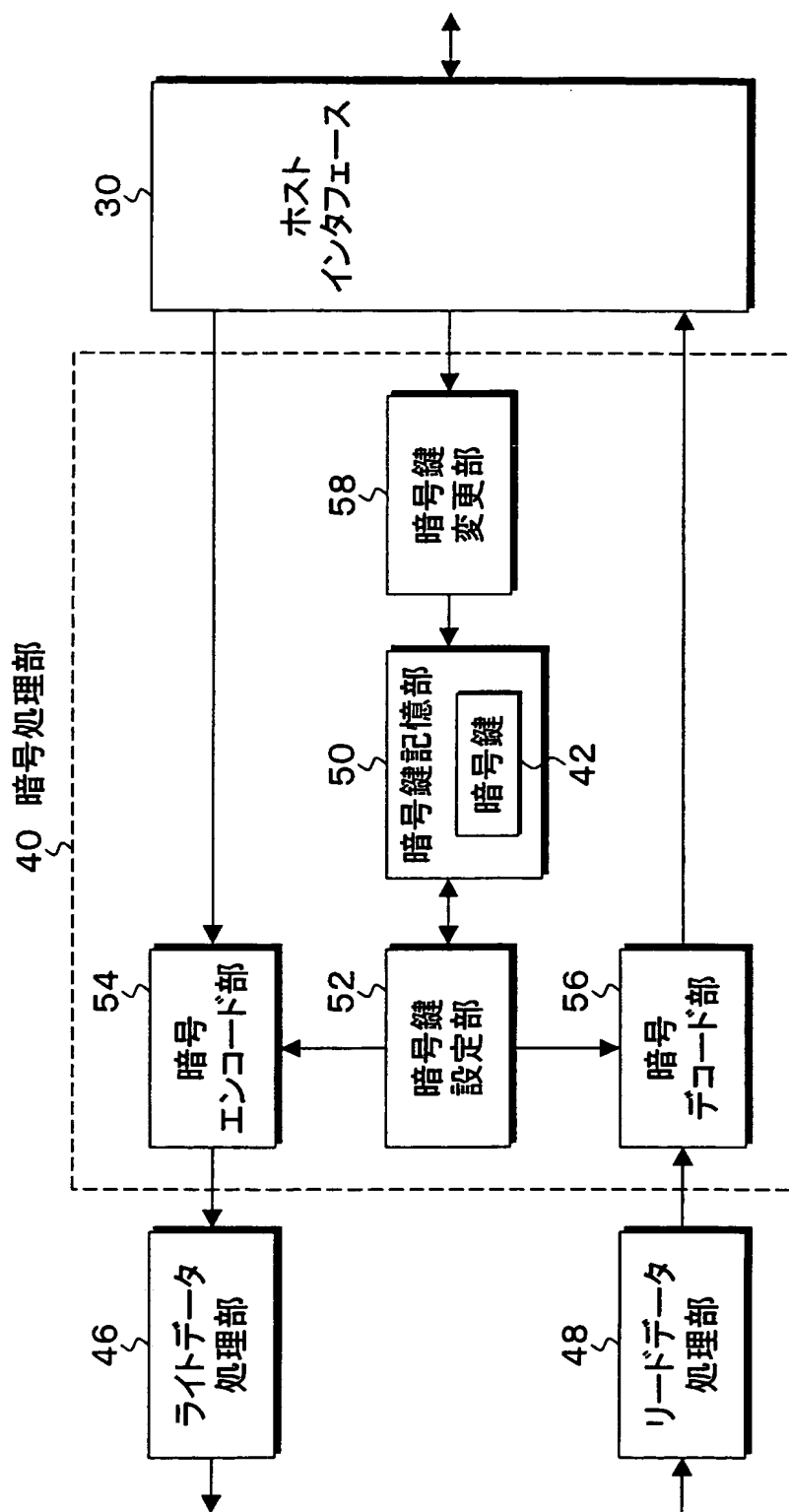
【図 3】

プログラムで暗号処理を行う本発明による磁気ディスク装置のブロック図



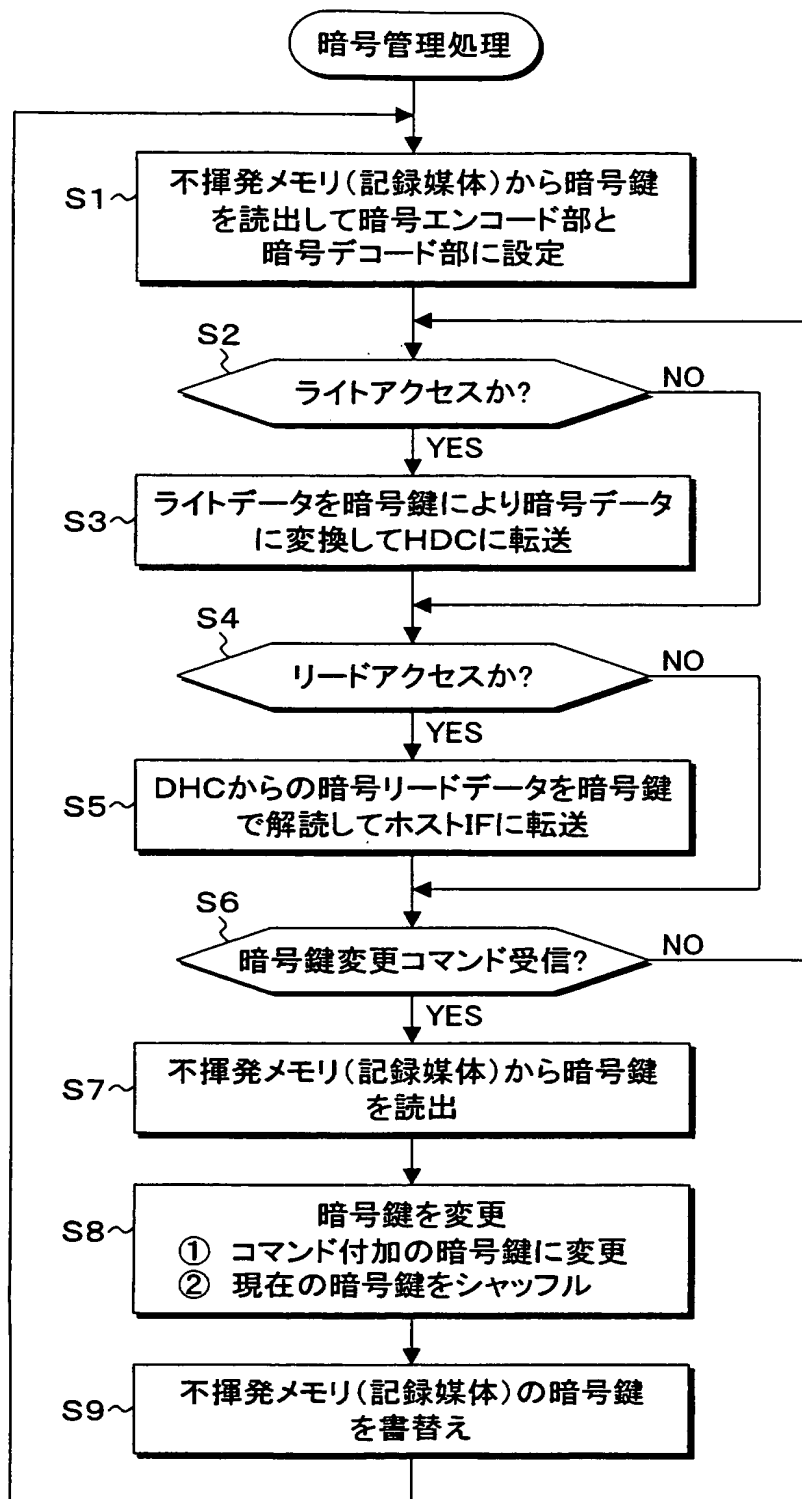
【図 4】

本発明によるプログラム暗号処理の機能構成のブロック図



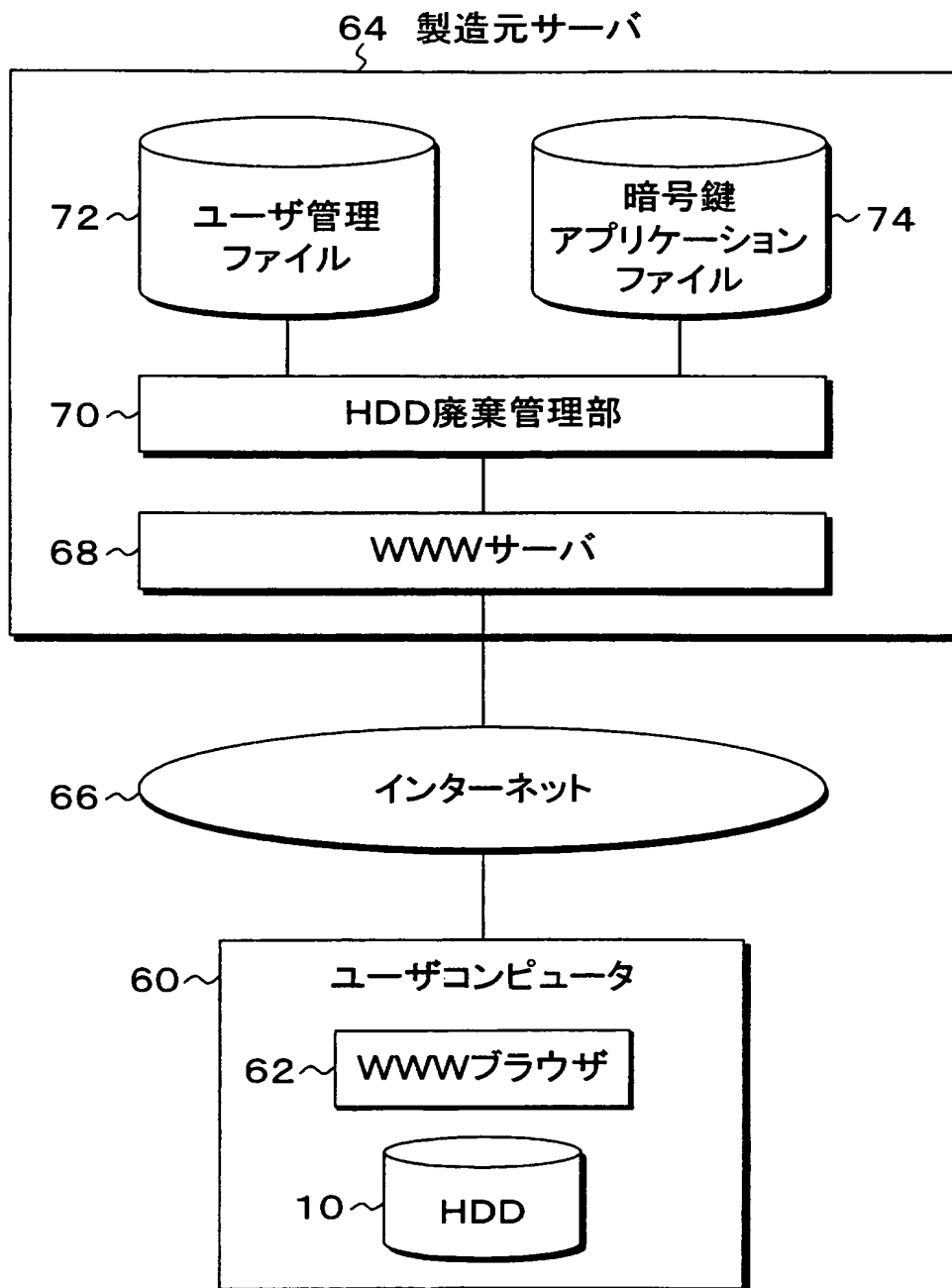
【図 5】

本発明における暗号処理のフローチャート



【図 6】

本発明の磁気ディスク装置に対し暗号鍵変更ツールを提供する
ネットワーク環境の説明図



【図 7】

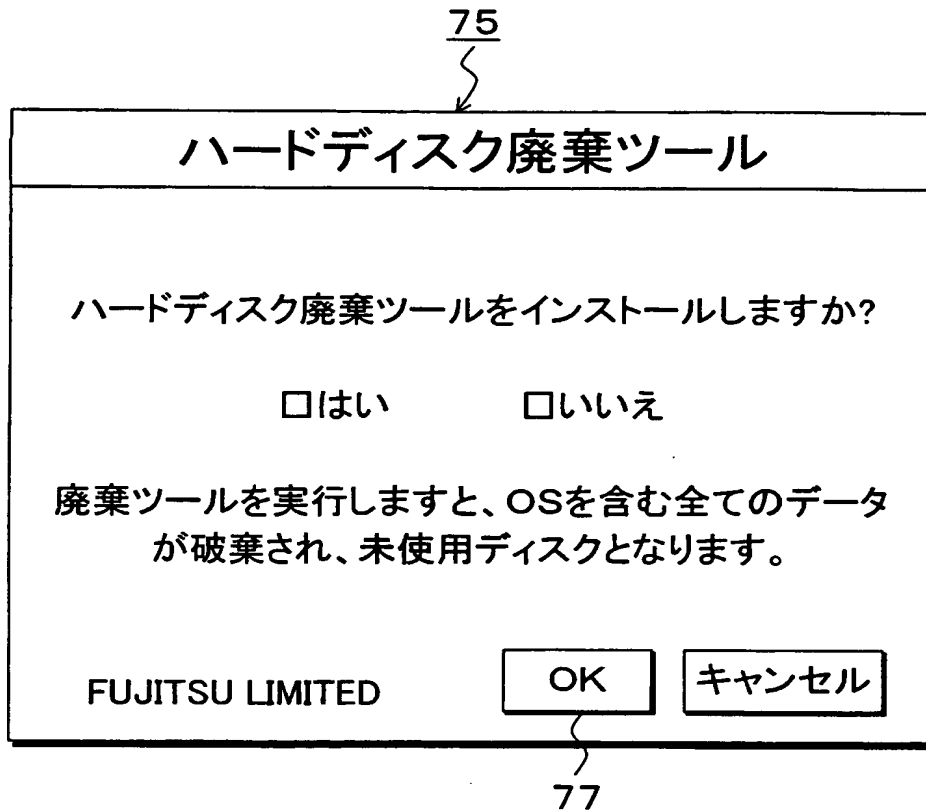
図6の製造元サーバにおけるユーザ管理ファイルの説明図

72

管理ID	コンピュータ番号	ハードディスク番号	暗号鍵 変更フラグ
0300001	FJ1234567890	HDD0000000100	0
0300002	FJ1234567891	HDD0000000101	0
0300003	FJ1234567892	HDD0000000102	0
0300004	FJ1234567893	HDD0000000103	1
0300005	FJ1234567894	HDD0000000104	0
0300006	FJ1234567895	HDD0000000105	0

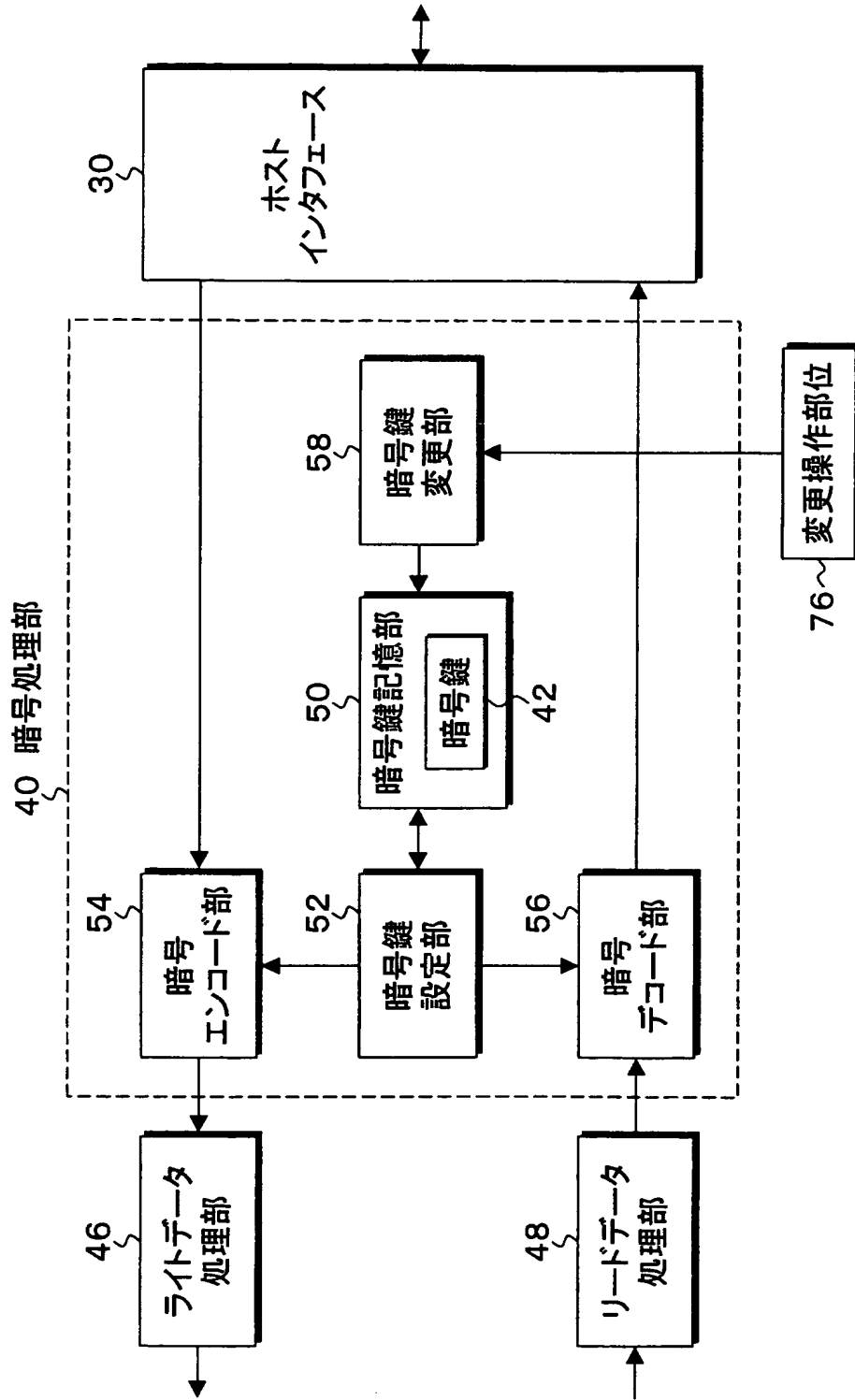
【図 8】

図6のブラウザにインストールしたハードディスク廃棄ツールの
の操作画面の説明図



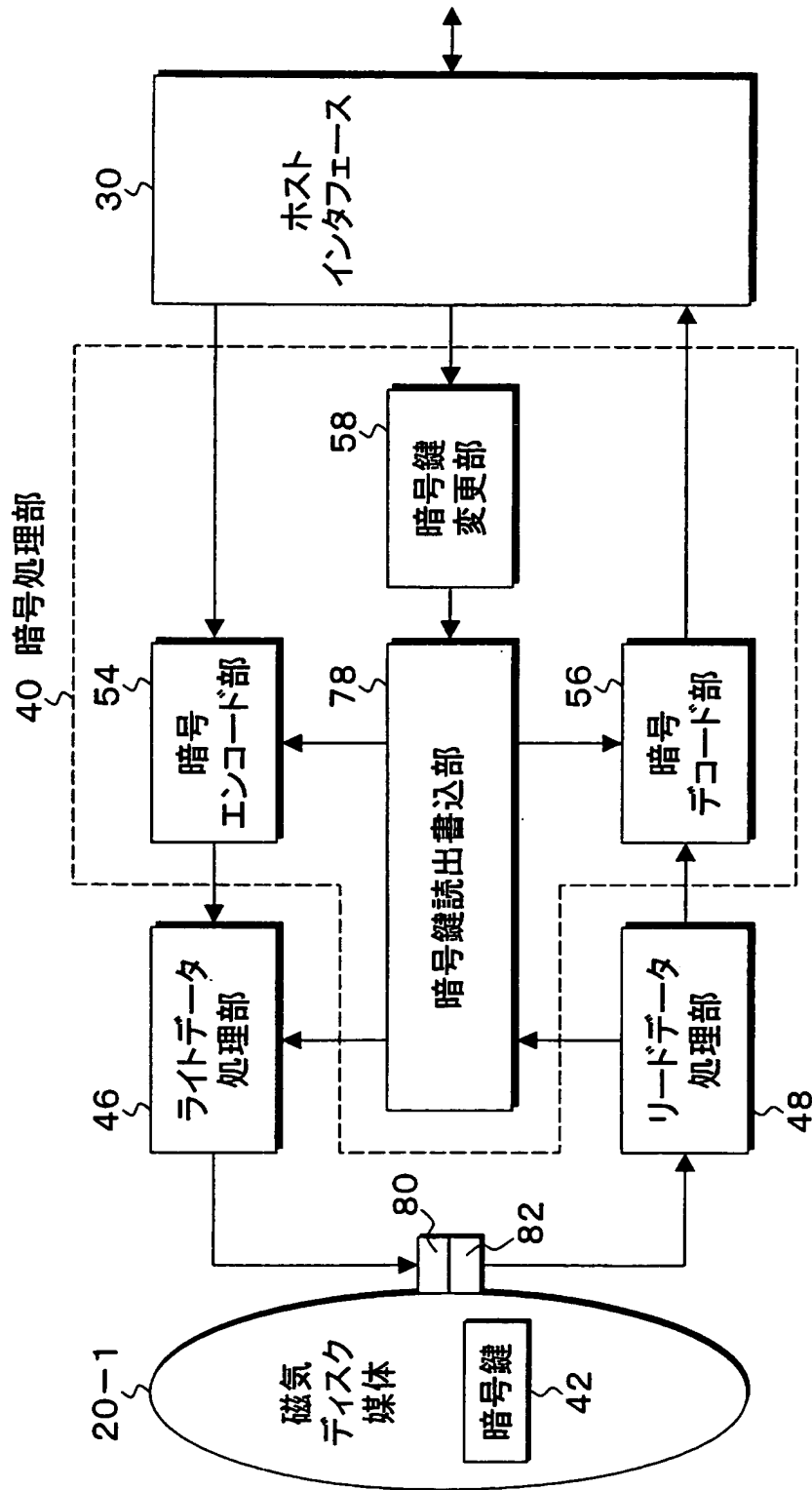
【図 9】

装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図



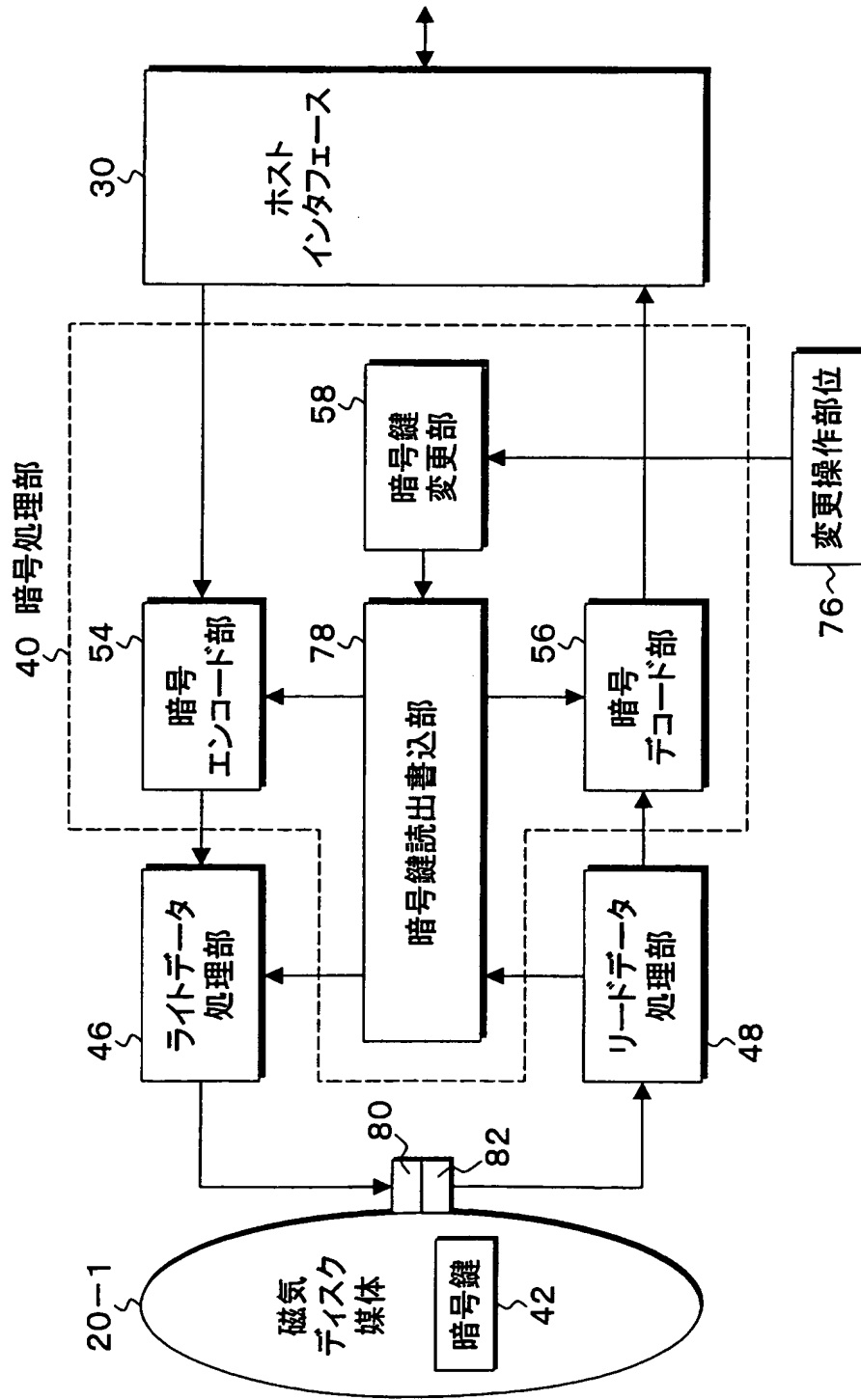
【図 10】

暗号鍵を記録媒体に格納した本発明の他の実施形態のブロック図



【図 11】

暗号鍵を記録媒体に格納し装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図



【書類名】 要約書

【要約】

【課題】 暗号化技術を利用して簡単且つ確実にデータ流出を防止する。

【解決手段】 暗号鍵記憶部 50 にデータの暗号化と復元に使用する暗号鍵 42 を記憶させる。暗号エンコード部 54 はホストインタフェース 30 を介して上位装置から入力されたデータを暗号鍵 42 を用いて暗号化して記録媒体に記録させる。暗号デコード部 56 は記録媒体から読み出された暗号データを暗号鍵 42 を用いて復元してホストインタフェース 30 より上位装置にデータを出力させる。磁気ディスク装置を廃棄する際には、暗号鍵変更部 58 により暗号鍵記憶部 50 に記憶されている暗号鍵 42 を変更して復元不能とする。

【選択図】 図 1

特願 2 0 0 3 - 1 3 6 8 6 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社